Exhibit 4

Cellular Communication Technologies LLC v. HTC Corp., et al

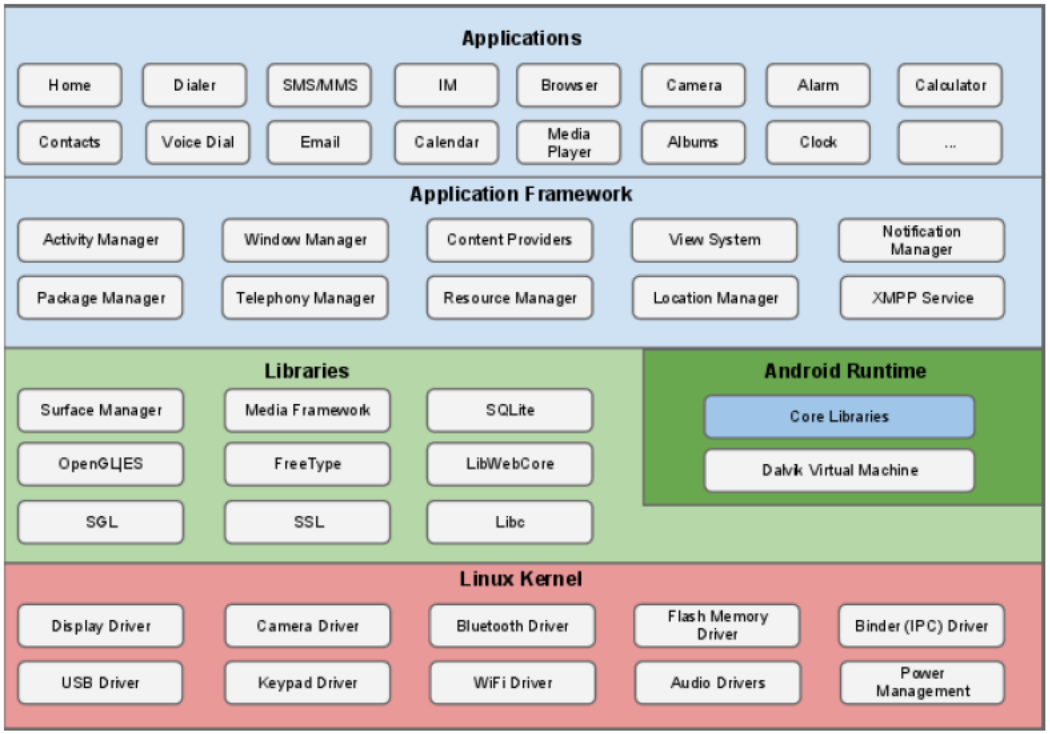
EXHIBIT F TO PLAINTIFF'S ~~FIRST~~SECOND SUPPLEMENTAL INFRINGEMENT CONTENTIONS

U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
24. A terminal for a communication system, the terminal comprising:	HTC, AT&T, Verizon, Sprint, and T-Mobile directly infringe the '8923 patent. Each Defendant makes, uses, sells, offers to sell, and/or imports the '8923 HTC Accused Products[2], each of which is a cellular device or tablet that includes the features and capabilities described in this claim. Plaintiff contends that each Defendant directly infringes this claim because it makes, uses, sells, offers to sell, and/or imports the '8923 HTC Accused Products, each of which includes each and every element of this claim. Each '8923 HTC Accused Product is a terminal for a communication system. Each Accused Product operates using the Android Operating System, and includes at least one application program configured to send messages towards a communication network, using, for example, SMS or MMS messaging functionality. Such an application program may be a native SMS/MMS program provided by the Android OS, or it may include other third party applications which are configured to send messages toward a communication network. For example, third party applications such as Handcent are also configured to send messages towards a communication network. The Android OS further contains a diverting unit that is part of the Application Framework of the operating system. In order for third party applications or the native messaging app to send text messages using the Android OS, these applications utilize the android.telephony API and call, for example, the sendTextMessage or sendMultipartTextMessage methods of the SMSManager

[1] Discovery in this case is ongoing. Accordingly, Plaintiff expects that these contentions may be subject to supplementation and/or amendment after further discovery and disclosure of Defendant's non-infringement positions in order to focus the issues in this case. For example, Plaintiff may supplement these contentions in response to information learned during discovery to rebut allegations of non-infringement under the doctrine of equivalents. Additionally, Plaintiff expects that these contentions may be subject to amendment or supplementation to identify and accuse additional devices released, developed, or made available after the date on which these contentions are served.

[2] The '8923 HTC Accused Products include the following products: HTC First, HTC One LTE, HTC One X+, HTC One mini, HTC One X LTE, HTC One max, HTC One SV, HTC Desire, HTC Desire 510, HTC Desire 610, HTC Desire 816, HTC One E8, HTC One M8, and HTC One Remix. Evidence supporting the use of relevant technology contained within this chart is listed in Appendix F-1.

U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
	class. Publicly available Google source code indicates that the SmsUsageMonitor.java is configured to limit the number of SMS/MMS messages an app can send in a particular period. This class controls the application based on the claimed criteria.
an application program configured to send messages towards a communication network;	Each '8923 HTC Accused Product operates using the Android Operating System, and includes at least one application program configured to send messages towards a communication network, using, for example, SMS or MMS messaging functionality. Such an application program may be a native SMS/MMS program provided by the Android OS (e.g. the "Messaging" app), or it may include other third party applications which are configured to send messages toward a communication network. For example, third party applications such as Handcent are also configured to send messages towards a communication network.
and a diverting unit configured to divert a message of the messages sent from the application program and destined for the communication network to a controlling entity residing in the terminal,	Each '8923 HTC Accused Product contains a diverting unit configured to divert a message of the messages sent from the application program and destined for the communication network to a controlling entity residing in the terminal. More specifically, the Android OS contains a diverting unit (e.g. the Telephony Manager) that is part of the Application Framework of the operating system. In order for third party applications or the native messaging app to send text messages using the Android OS, these applications utilize the android.telephony API and call, for example, the sendTextMessage or sendMultipartTextMessage methods of the SMSManager class. The diverting unit (i.e. the Telephony Manager) diverts a message of the messages sent when the respective method calls are made by the application. The message is diverted to a controlling entity

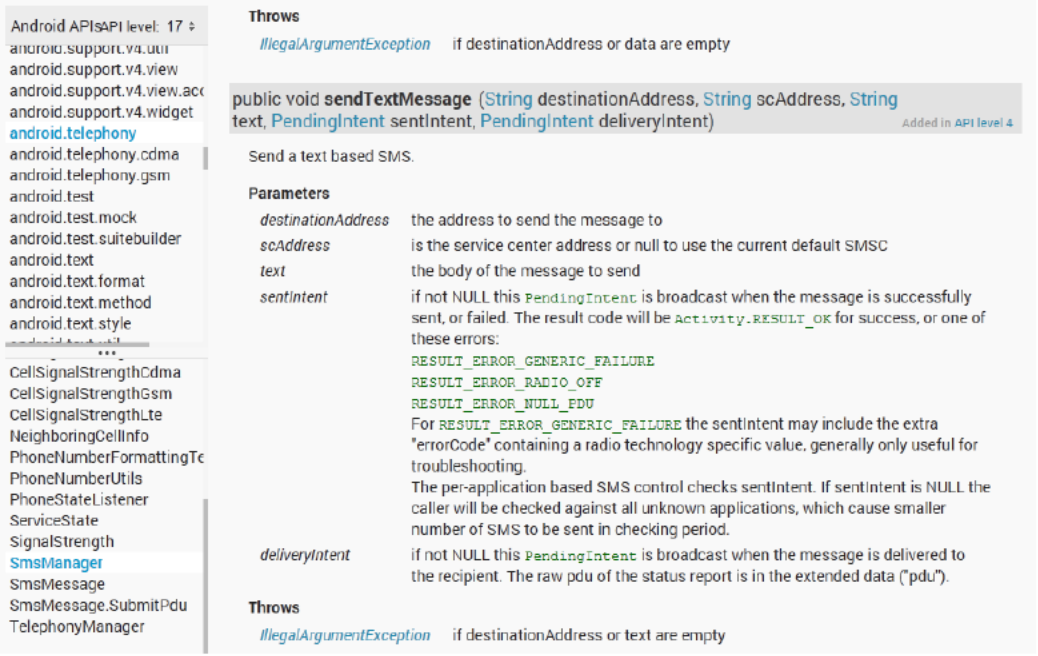
U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
	called the SmsUsageMonitor which acts as a controlling entity and resides in the terminal as part of the Android OS. [3,4] 

[3] See http://source.android.com/tech/security/

[4] See http://developer.android.com/reference/android/telephony/SmsManager html

Cellular Communication Technologies LLC v. HTC Corp., et al

EXHIBIT F TO PLAINTIFF'S ~~FIRST~~SECOND SUPPLEMENTAL INFRINGEMENT CONTENTIONS

U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
	 Alternatively, CCE contends that this claim element is met under the doctrine of equivalents because above-described features of the Accused Products perform substantially the same function recited in this element, in substantially the same way to achieve substantially the same result. Any alleged differences between the above-described features and the recited element are insubstantial and immaterial to infringement.
wherein the controlling entity is configured to control, based on the message and before the message is transmitted to the communication network, whether the application program behaves in a predetermined manner in the	The controlling entity is configured to control, based on the message and before the message is transmitted to the communication network, whether the application program behaves in a predetermined manner in the communication terminal. Namely, the SmsUsageMonitor determines whether the application program has sent too many messages in a given time period. If, for example, the application

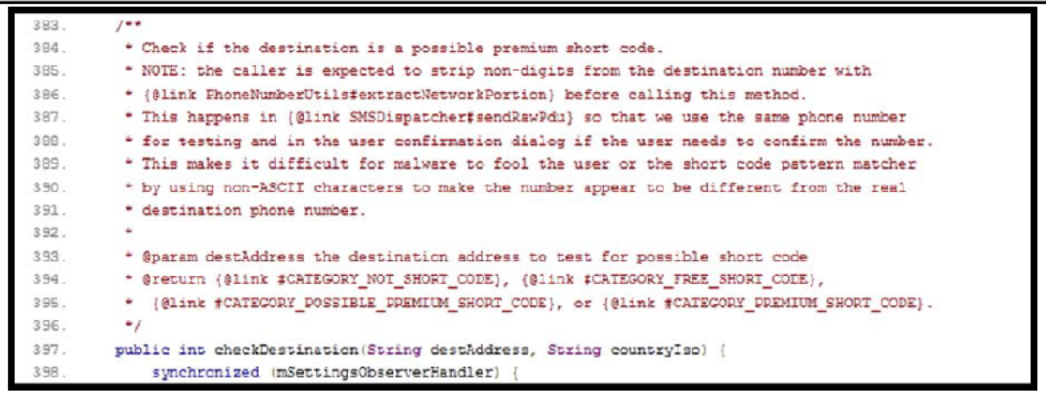
U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
communication terminal,	attempts to send too many messages within a certain period, the SmsUsageMonitor will warn the user before the message is transmitted. In the alternative, the SmsUsageMonitor will determine if the message is being sent to a premium SMS short code. If the message is destined for a premium SMS short code, the controlling entity will require seek confirmation from the user before the message is transmitted.[5]

```
58.
59. /**
60.  * Implement the per-application based SMS control, which limits the number of
61.  * SMS/MMS messages an app can send in the checking period.
62.  *
63.  * This code was formerly part of {@link SMSDispatcher}, and has been moved
64.  * into a separate class to support instantiation of multiple SMSDispatchers on
65.  * dual-mode devices that require support for both 3GPP and 3GPP2 format messages.
66.  */
67. public class SmsUsageMonitor {
68.     private static final String TAG = "SmsUsageMonitor";
69.     private static final boolean DBG = false;
70.     private static final boolean VDBG = false;
71.
72.     private static final String SHORT_CODE_PATH = "/data/misc/sms/codes";
73.
74.     /** Default checking period for SMS sent without user permission. */
75.     private static final int DEFAULT_SMS_CHECK_PERIOD = 60000;      // 1 minute
76.
77.     /** Default number of SMS sent in checking period without user permission. */
78.     private static final int DEFAULT_SMS_MAX_COUNT = 30;
```

[5] See https://android.googlesource.com/platform/frameworks/opt/telephony/+/master/src/java/com/android/internal/telephony/SmsUsageMonitor.java

Cellular Communication Technologies LLC v. HTC Corp., et al

EXHIBIT F TO PLAINTIFF'S ~~FIRST~~SECOND SUPPLEMENTAL INFRINGEMENT CONTENTIONS

U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
	 ``` /** * Check if the destination is a possible premium short code. * NOTE: the caller is expected to strip non-digits from the destination number with * {@link PhoneNumberUtils#extractNetworkPortion} before calling this method. * This happens in {@link SMSDispatcher#sendRawPdu} so that we use the same phone number * for testing and in the user confirmation dialog if the user needs to confirm the number. * This makes it difficult for malware to fool the user or the short code pattern matcher * by using non-ASCII characters to make the number appear to be different from the real * destination phone number. * * @param destAddress the destination address to test for possible short code * @return {@link #CATEGORY_NOT_SHORT_CODE}, {@link #CATEGORY_FREE_SHORT_CODE}, * {@link #CATEGORY_POSSIBLE_PREMIUM_SHORT_CODE}, or {@link #CATEGORY_PREMIUM_SHORT_CODE}. */ public int checkDestination(String destAddress, String countryIso) { synchronized (mSettingsObserverHandler) { ``` Alternatively, CCE contends that this claim element is met under the doctrine of equivalents because above-described features of the Accused Products perform substantially the same function recited in this element, in substantially the same way to achieve substantially the same result. Any alleged differences between the above-described features and the recited element are insubstantial and immaterial to infringement.
and wherein the terminal is a terminal of a communications system.	Each '8923 HTC Accused Product is either a tablet device with messaging capabilities or a cellular device with messaging capabilities. The messaging capabilities of both of these classifications of devices mean that each accused product is a terminal of a communications system.
26. The terminal according to claim 24, wherein the controlling entity is configured to reside in a tamper resistant area of the terminal.	See analysis of claim 24, which is incorporated herein by reference. Each of the '8923 HTC Accused Products contains a controlling entity which is configured to reside in a tamper resistant area of the terminal. Specifically, the controlling entity is the SmsUsageMonitor and is configured to execute as part of the Android operating system. The Android operating system utilizes an Application Sandbox approach to prevent unauthorized access to processes. Such security is kernel level security and prevents applications from interfering with one another, but also prevents applications from accessing objects that execute as

U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
	part of the operating system itself without explicit permission to do so.[6] Thus, the controlling entity resides in a tamper resistant area of the terminal. **The Application Sandbox** The Android platform takes advantage of the Linux user-based protection as a means of identifying and isolating application resources. The Android system assigns a unique user ID (UID) to each Android application and runs it as that user in a separate process. This approach is different from other operating systems (including the traditional Linux configuration), where multiple applications run with the same user permissions. This sets up a kernel-level Application Sandbox. The kernel enforces security between applications and the system at the process level through standard Linux facilities, such as user and group IDs that are assigned to applications. By default, applications cannot interact with each other and applications have limited access to the operating system. If application A tries to do something malicious like read application B's data or dial the phone without permission (which is a separate application), then the operating system protects against this because application A does not have the appropriate user privileges. The sandbox is simple, auditable, and based on decades-old UNIX-style user separation of processes and file permissions. Since the Application Sandbox is in the kernel, this security model extends to native code and to operating system applications. All of the software above the kernel in *Figure 1*, including operating system libraries, application framework, application runtime, and all applications run within the Application Sandbox. On some platforms, developers are constrained to a specific development framework, set of APIs, or language in order to enforce security. On Android, there are no restrictions on how an application can be written that are required to enforce security; in this respect, native code is just as secure as interpreted code. In some operating systems, memory corruption errors generally lead to completely compromising the security of the device. This is not the case in Android due to all applications and their resources being sandboxed at the OS level. A memory corruption error will only allow arbitrary code execution in the context of that particular application, with the permissions established by the operating system. Like all security features, the Application Sandbox is not unbreakable. However, to break out of the Application Sandbox in a properly configured device, one must compromise the security of the the Linux kernel. **System Partition and Safe Mode** The system partition contains Android's kernel as well as the operating system libraries, application runtime, application framework, and applications. This partition is set to read-only. When a user boots the device into Safe Mode, only core Android applications are available. This ensures that the user can boot their phone into an environment that is free of third-party software. **Filesystem Permissions** In a UNIX-style environment, filesystem permissions ensure that one user cannot alter or read another user's files. In the case of Android, each application runs as its own user. Unless the developer explicitly exposes files to other applications, files created by one application cannot be read or altered by another application.
32. The terminal according to claim 24, wherein the terminal comprises a mobile	See analysis of claim 24, which is incorporated herein by reference.

[6] See http://source.android.com/tech/security/

Cellular Communication Technologies LLC v. HTC Corp., et al

EXHIBIT F TO PLAINTIFF'S ~~FIRST~~SECOND SUPPLEMENTAL INFRINGEMENT CONTENTIONS

U.S. Pat. No. 7,218,923	'8923 HTC ACCUSED PRODUCTS[1]
terminal.	Each of the '8923 HTC Accused Products comprises a mobile terminal such as a tablet or a cellular phone device.